UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/916,714	07/26/2001	Neil John Hursey	NAI1P016/01.065.01	8235

28875 7590 04/11/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
AMSBURY, WAYNE P	

ART UNIT	PAPER NUMBER
2161	

DATE MAILED: 04/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/916,714	HURSEY ET AL.	
	Examiner	Art Unit	
	Wayne Amsbury	2161	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 February 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,7,8,10-14,20,21 and 23-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,7,8,10-14,20,21 and 23-33* is/are rejected.

7)☒ Claim(s) *34* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

TL

CLAIMS 1,7,8,10-14,20,21 AND 23-34 ARE PENDING

1. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

2. Applicant's arguments with respect to claims 1,7,8,10-14,20,21 and 23-28 have been considered but are moot in view of the new ground(s) of rejection.

The amendments have shifted limitations from dependent claims to independent claims without materially changing the invention as examined. In the interest of compact prosecution the arguments directed to the tree-like nature of indexes and the basic format of tree structures are addressed here by applying prior art that provides explicit teachings about those aspects of computer science.

New claims 29-34 present further limitations not present in the original claims, but this rejection is made non-final in order to explicitly address basic elements of computer science as noted above.

3. **Claims 1,8,10-14,20,21, 23-29 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Radatti, US 20020170052, 14 November 2002 and Corman et al (Corman), Introduction to Algorithms, the MIT Press, 1986, Section 5.5, pp. 91-97 and Chapter 13, pp. 244-262.**

Radatti is directed to data transmission of antivirus software in order to update a virus signature database that is used to recognize virus code [001], [005].

As to **claim 1**:

identifying a list of virus signatures

The virus signature database corresponds to a list of virus signatures, and an update_index file that may contain a plurality of updates [see below] is an index of files containing signatures.

combining the list of virus signatures into a tree of virus signatures

In some embodiments of Radatti the update_index file is referential and organized into a tree [0034], [0047]. Such an index organizes the underlying data into a tree determined by access to it via the index.

comparing data against the tree of virus signatures for virus signature recognition

This is taught at least in FIG 1 box **11**. In more detail:

wherein the virus signatures each include a sequence of characters

The data transmitted, including upgrades to virus signatures may be a sequence of characters [0011].

wherein the tree includes a plurality of branches each including a sequence of characters

It is the nature of a tree with more than one node to include a plurality of branches. Radatti does not explicitly teach this and some other limitations noted below that were so well known to practitioners of the art that no explicit teaching is required.

However, Corman is a freshman text that teaches the basic nature of trees in general, and search trees that correspond to database indexes in particular.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the standard treatments of trees as taught by Corman into the index trees of Radatti because it is efficient to incorporate a well known body of knowledge instead of developing a new one.

Corman provides evidence of the plurality of branches of trees in the basic discussion of trees, Section 5.5, pp. 91-97, in particular FIG 5.7 page 95, and search trees such as the indexes of Radatti in Chapter 13, pp. 244-262.

wherein a portion of the branches corresponds to a plurality of the virus signatures

This is clearly an aspect of the referential update_index file structure noted above [0034], [0047].

wherein the efficiency of the virus signature recognition is improved by reducing an amount of virus signature data that is compared against the data

This is the nature of both an index and a hash function, and of a search tree in general. See also the discussion of search the search time advantages of binary search trees, Corman page 244.

wherein the branches include upper branch portions and lower branch portions

See Corman, FIG 5.6 page 94; FIG 13, page 245.

As to **claim 8**, *wherein the characters of the tree of virus signatures are obfuscated to prevent detection by the comparison.*

The hash function included in the update_index is a form of obfuscation [0024]-[0033].

As to **claims 10-12**: *wherein the comparing includes comparing the data against the upper branch portions of the tree.*

This is the nature of the tree walk of a search tree such as the update_index of Radatti. See Corman page 245 and after.

As to **claim 13**: *wherein data is eligible to be declared clean upon the unsuccessful comparison of the data against an entirety of at least one branch that includes all of the characters of one of the virus signatures*

This is simply the consequence of reaching a leaf node of a search tree of virus signatures without finding a virus. It is the nature of such a search that a failure to find any matching virus signature indicates that there is none to the extent that the database can be used for the determination.

The elements of claims **14, 20, 21 and 23-29** are rejected in the analysis above and these claims are rejected on that basis.

As to **claim 31**, both the formation of an update_index and hashing comprise pre-processing.

4. **Claims 7, 30 and 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Radatti, US 20020170052, 14 November 2002 and Corman et al (Corman), Introduction to Algorithms, the MIT Press, 1986, Section 5.5, pp. 91-97 and Chapter 13, pp. 244-262 in further view of Arnold, US 5,440,712, 8 August 1995.**

Neither Radatti nor Corman teach the use of wildcards during virus detection, but Arnold does so.

As to **claim 7**, Arnold teaches the use of wildcards during virus detection [COL 11 lines 53-60] and in more particular, that they can be added to existing virus detection software [COL 14 lines 31-48].

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate wildcards into the virus detection software of Radatti because adds robustness to variations in a virus.

As to **claims 30 and 32-33**, Arnold teaches the well-known use of the exclusive-OR operation, virus location within a file, reduction of virus portion compared, decryption, and emulation in the context of virus detection [COL 8 lines 17-60; COL 13 lines 52-67].

5. **Claim 34 is objected to** as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

While it is considered that this limitation is within the purview of a programmer of ordinary skill in the art, it is neither inherent nor obvious on the basis of the prior art of record.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Wayne Amsbury whose telephone number is 571-272-4015. The examiner can normally be reached on M-F 6-18:30 FIRST WEEK.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Safet Metjahic can be reached on 571-272-4023. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

WPA

WAYNE AMSBURY
PRIMARY PATENT EXAMINER